



## DEPARTMENT OF ENERGY

### Federal Energy Regulatory Commission

#### Privacy Act of 1974; System of Records

**AGENCY:** Federal Energy Regulatory Commission, Department of Energy.

**ACTION:** Notice of a modified system of records.

**SUMMARY:** The Federal Energy Regulatory Commission (FERC) is publishing a notice of modifications to an existing FERC system of records, FERC-35 titled Commission Security Investigation Records. In accordance with the Privacy Act of 1974, and to comply with the Office of Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017, this notice will create 9 new routine uses, and will incorporate two new routine uses that permit FERC to disclose information as necessary in response to an actual or suspected breach that pertains to a breach of its own records or to assist another agency in its efforts to respond to a breach that were previously published separately in the *Federal Register* of July 11, 2023. This System of Records Notice (SORN) also describes the way in which security investigations on FERC employees, applicants for FERC employment, and individuals performing work for the Commission under contract, is conducted.

**DATES:** In accordance with 5 U.S.C. section 552a(e)(4) and (11), this system of records notice is effective upon publication, with the exception of the routine uses, which will go into effect 30 days after publication of this notice, unless comments have been received from interested members of the public requiring modification and republication of the notice.

**ADDRESSES:** Any person interested in commenting on the establishment of this modified system of records may do so by submitting comments in writing to: [Privacy@ferc.gov](mailto:Privacy@ferc.gov) (Include reference to “Commission Security Investigations Records—FERC-35” in the subject line of the message.)

For United States Postal Service-delivered mail: Director, Office of the Secretary (OSEC)

Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426.

For hand-delivered or courier-delivered mail: Director, Office of External Affairs, Federal

Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852.

**FOR FURTHER INFORMATION CONTACT:** Mittal Desai, Chief Information Officer & Senior Agency Official for Privacy, Office of the Executive Director Office of the Executive Director 888 First Street, NE Washington, DC. 20426, (202) 502–6432.

**SUPPLEMENTARY INFORMATION:** The FERC Commission Security Investigations Records notice has 9 new routines and includes two prescribed routine uses that permit FERC to disclose information as necessary in response to an actual or suspected breach that pertains to a breach of its own records or to assist another agency in its efforts to respond to a breach that were previously published in the *Federal Register* of July 11, 2023 (87 FR 35543, entitled Notice of Modified System of Records for PII Breach Response Routine Uses).

**SYSTEM NAME AND NUMBER:** Commission - FERC-35.

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Federal Energy Regulatory Commission, Chief Security Officer Directorate, 888 First Street, NE, Room 3A - 09, Washington, DC 20426.

**SYSTEM MANAGER(S):** Chief Security Officer Directorate, Federal Energy Regulatory Commission, 888 First Street, NE, Room ED - 43, Washington, DC 20426.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 5 U.S.C. 301, 2302(b)(2)(B), 2302(b)(10), 7311, 7313; Executive Order 13764; 5 CFR 731.103, 18 CFR 3b.

**PURPOSE(S) OF THE SYSTEM:** The records in this system are used to provide investigative and related administrative, adjudicative, and other information necessary to determine whether an individual is suitable or fit for Government employment; eligible for physical access to FERC controlled facilities and information systems; eligible to hold sensitive positions (including but not limited to eligibility for access to classified information); fit to perform work for or on behalf

of the U.S. Government as a contractor; qualified to perform contractor services for the U.S. Government; or loyal to the United States; while maintaining compliance with applicable legal, regulatory and policy authorities.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Current and former FERC employees, contractors, interns, volunteers, as well as other individuals (including contractor personnel of other Government entities and foreign nationals) requiring a FERC determination for suitability or fitness for duty, HSPD-12 access, access to classified national security information, Sensitive Compartmented Information, and/or assignment to a position with sensitive duties; and officials or employees of State, local, tribal and private sector entities sponsored for access to classified and other sensitive information by a Federal agency.

**CATEGORIES OF RECORDS IN THE SYSTEM:** This system maintains information collected as part of the investigative vetting process. This information may include the individual's personally identifiable information; residential, educational, employment, and mental health history; financial details, and criminal and disciplinary histories; to include: Current, former, alternate name, social security number, home and work address and phone number, reference's home and work address and phone number. Additional information collected may include date of birth; place of birth; height; weight; hair and eye color; gender; sex; mother's maiden name; residential history, phone numbers, and email addresses; employment history; military records and discharge information; selective service registration record; educational data, including conduct records and degrees earned; names of relatives, associates and references with their contact information; country/countries of citizenship; travel, immigration, and passport information; mental health history; records related to drug and/or alcohol use; financial record information; information pertaining to income tax returns; bureau of vital statistics records (e.g., birth certificate, death certificate, marriage application and license); credit reports; prior security clearance and investigative information; employing activity; current employment status; position sensitivity; personnel security investigative basis; status of current

adjudicative action; security clearance eligibility status and access status; self-reported information; eligibility recommendations or decisions made by an appellate authority; inadvertent disclosure briefing and agreement; non-disclosure execution dates; indoctrination date(s); level(s) of access granted; briefing/debriefing date(s) and reasons for briefing/debriefing; and other biographical information as required during the course of a background investigation. In addition, this system may contain records documenting the outcomes of investigations and adjudications conducted by other Federal investigative organizations (e.g., U.S. Office of Personnel Management (OPM), Federal Bureau of Investigation, Department of Defense, etc.) and locator references to such investigations. Entries documenting fitness determinations, HSPD-12 access, continuous vetting adverse information flags, or counter insider threat reports of the subject and investigative information for spouse or cohabitant(s); the name and marriage information for current and/or former spouse(s); the country/countries of citizenship, name, date, and place of birth, contact information (e.g., phone numbers, email addresses), and address for relatives. Reports from pre-employment screening, such as counterintelligence screening or military accessions vetting; results of subject and reference interviews conducted during background investigations, continuous evaluation, counter insider threat, counterintelligence screening, security incident resolution, or program access requests. Information detailing agency investigation requests including type of investigation requested, tracking codes, and requesting officials' contact information. Biometric information including but not limited to images and fingerprints, criminal and civil fingerprint history information. Foreign contact, affections, associates (e.g., family members, friends or social contacts), travel, and activities information, including names of individuals known, dates, country/countries of citizenship, country/countries of residence, type and nature of contact, financial interests, assets, benefits from foreign governments, countries and dates of arrival and departure for U.S. border crossings; association records; information on loyalty to the United States. Criminal history information, including information contained in local, State, military, Federal, and foreign criminal justice agency

records and local, State, military, and Federal civil and criminal court records. Information about affiliation with known criminal and/or terrorist organizations. Records concerning civil or administrative proceedings, (for example, bankruptcy records, civil lawsuits, Merit System Protection Board), including information contained in local, State, military, Federal, and foreign courts, and agency records. Information about and evidence of unauthorized use or misuse of information technology systems. Information aggregated in counter-insider threat inquiries or investigations, including payroll information, travel vouchers, benefits information, equal employment opportunity complaints, performance evaluations, disciplinary files, training records, substance abuse and mental health records of individuals undergoing law enforcement action or presenting an identifiable imminent threat, counseling statements, outside work and activities requests, and personal contact records; particularly sensitive or protected information, including information held by special access programs, law enforcement, inspector general, or other investigative sources or programs. Agency or Component summaries of reports, and full reports, about potential insider threats from records of usage of Government telephone systems, including the telephone number initiating the call, the telephone number receiving the call, and the date and time of the call. U.S. and foreign finance and real estate information that consists of names of financial institutions, number of accounts held, monthly and year-end account balances for bank and investment accounts, address, year of purchase and price, capital investment costs, lease or rental information, year of lease or rental, monthly payments, deeds, lender/loan information and foreclosure history; information on owned and leased vehicles, boats, airplanes and other U.S. and foreign assets that include type, make, model, year, plate or identification number, year leased, monthly rental payment; year of purchase and price, and fair market value; information pertaining to large or suspicious currency transactions; U.S. and foreign mortgages, loans, and liabilities information that consist of type of loan, names and addresses of creditors, original balance, monthly and year-end balance, monthly payments, and payment history. Publicly available electronic information about or generated by a covered individual (e.g., public

records, civil court records, social media content, news articles, and web blog information).

Results of record checks and data analyses for purposes of improving all types of investigations, reinvestigations, or continuous evaluation with respect to efficiency or cost effectiveness.

**RECORD SOURCE CATEGORIES:** Records are obtained from individual employees, applicants, consultants, experts and contractors (including the results of in-person interviews) whose files are on record as authorized by those concerned; investigative reports from Federal investigative agencies; criminal or civil investigations; continuous evaluation records; police and credit record checks; personnel records; educational records and instructors; current and former employers; coworkers, neighbors, family members, acquaintances; and authorized security representatives.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING**

**CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, information maintained in this system may be disclosed to authorized entities outside FERC for purposes determined to be relevant and necessary as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To appropriate agencies, entities, and persons when (1) FERC suspects or has confirmed that there has been a breach of the system of records; (2) FERC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

To another Federal agency or Federal entity, when FERC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the

risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

To the Equal Employment Opportunity Commission (EEOC) when requested in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law or regulation.

To the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.

To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding. In those cases where the Government is not a party to the proceeding, records may be disclosed if a subpoena has been signed by a judge.

To the Department of Justice (DOJ) for its use in providing legal advice to FERC or in representing FERC in a proceeding before a court, adjudicative body, or other administrative body, where the use of such information by the DOJ is deemed by FERC to be relevant and necessary to the advice or proceeding, and such proceeding names as a party in interest: (a) FERC; (b) any employee of FERC in his or her official capacity; (c) any employee of FERC in his or her individual capacity where DOJ has agreed to represent the employee; or (d) the United States, where FERC determines that litigation is likely to affect FERC or any of its components.

To non-Federal Personnel, such as contractors, agents, or other authorized individuals performing work on a contract, service, cooperative agreement, job, or other activity on behalf of

FERC or Federal Government and who have a need to access the information in the performance of their duties or activities.

To the National Archives and Records Administration in records management inspections and its role as Archivist.

To the Merit Systems Protection Board or the Board's Office of the Special Counsel, when relevant information is requested in connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, and investigations of alleged or possible prohibited personnel practices.

To appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, if the information may be relevant to a potential violation of civil or criminal law, rule, regulation, order.

To the Department of Defense's Defense Counter Intelligence and Security Agency (DOD/DCSA), and other Departments and agencies that shares PII with FERC, in connection with the vetting of individuals (employees or applicants) for Federal employment, military service, consulting, volunteer personnel and/or contractor personnel, for national security purposes, including but not limited to, personnel background investigations, continuous vetting, suitability investigations and for satisfying the credentialing requirements of HSPD-12.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Records are maintained in electronic and paper format. Electronic records are stored by individuals first and last names. In addition, all FERC employees and contractors with authorized access have undergone a thorough background security investigation. Data access is restricted to agency personnel or contractors whose responsibilities require access. Access to electronic records is controlled by user ID and password combination and/or other network access or security controls (e.g., firewalls). Role based access is used to restrict electronic data access and the organization employs the principle of least privilege, allowing only authorized users with access (or processes acting on behalf of users) necessary to accomplish assigned tasks in accordance with organizational missions and



business functions. Paper records are maintained in combination safes in locked rooms pursuant to OPM regulations. Buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures. The system is secured with the safeguards required by NIST SP 800-53. Materials, including hard copy printouts derived from electronic records created on an ad hoc basis for reference purposes or to meet day-to-day business needs, are destroyed when the Commission determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records may be retrieved by name, social security number, date of birth, place of birth, Defense Counterintelligence and Security Agency [Investigative Service Provider] investigation number, adjudicative case identification number or some combination thereof.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** Records are retained under the National Archives and Records Administration's General Records Schedule 5.6: Security Management Records; Disposition Authority: DAA-GRS-2021-0001-0007). Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** All FERC employees and contractors with authorized access have undergone a thorough background security investigation. Data access is restricted to agency personnel or contractors whose responsibilities require access. Access to electronic records is controlled by "User ID" and password combination and/or other network access or security controls (e.g., firewalls). The system is secured with the safeguards required by FISMA and NIST SP 800-53. Physical access to FERC is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Paper records are maintained in combination safes in locked rooms pursuant to OPM regulations. Buildings are guarded and

monitored by security personnel, cameras, ID checks, and other physical security measures. The system is secured with the safeguards required by NIST SP 800-53.

## **RECORD ACCESS PROCEDURES:**

### **Submit a Privacy Act Request**

The Privacy Act permits access to records about yourself that are maintained by FERC in a Privacy Act system of records. In addition, you may request that incorrect or incomplete information be changed or amended.

Privacy requests follow FERC's Freedom of Information Act (FOIA) request process. You may access the FOIA website at <https://www.ferc.gov/freedom-information-act-foia-and-privacy-act>.

For questions: Contact the FOIA Service Center at 202-502-6088 or by email at [foia-ceii@ferc.gov](mailto:foia-ceii@ferc.gov). Written request for access to records should be directed to: Director, Office of External Affairs, Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426.

**CONTESTING RECORD PROCEDURES:** The Privacy Act permits access to records about yourself that are maintained by FERC in a Privacy Act system of records. In addition, you may request that incorrect or incomplete information be changed or amended. Privacy requests follow FERC's FOIA request process. You may access the FOIA website at

<https://www.ferc.gov/freedom-information-act-foia-and-privacy-act>. For questions: Contact the FOIA Service Center at 202-502-6088 or by email at [foia-ceii@ferc.gov](mailto:foia-ceii@ferc.gov). Written request for access to records should be directed to: For United States Postal Service-delivered mail:

Director, Office of External Affairs, Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426. For hand-delivered or courier-delivered mail: Director, Office of External Affairs, Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852.

**NOTIFICATION PROCEDURES:** The Privacy Act permits access to records about yourself that are maintained by FERC in a Privacy Act system of records. In addition, you may request

that incorrect or incomplete information be changed or amended. Privacy requests follow FERC's FOIA request process. You may access the FOIA website at <https://www.ferc.gov/freedom-information-act-foia-and-privacy-act>. For questions: Contact the FOIA Service Center at 202-502-6088 or by email at [foia-ceii@ferc.gov](mailto:foia-ceii@ferc.gov). Written request for access to records should be directed to: For United States Postal Service-delivered mail: Director, Office of External Affairs, Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426. For hand-delivered or courier-delivered mail: Director, Office of External Affairs, Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** 65 FR 21752.

Issued: April 3, 2023.

Kimberly D. Bose,  
Secretary.

[FR Doc. 2023-07288 Filed: 4/11/2023 8:45 am; Publication Date: 4/12/2023]